M. Anderson Berry (SBN 262879)
Leslie Guillon (SBN 222400)
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916)777-7777
Facsimile: (916) 924-1829
aberry@justice4you.com
lguillion@justice4you.com

John A. Yanchunis
(Pro Hac Vice application forthcoming)
Ryan D. Maxey
(Pro Hac Vice application forthcoming)
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin St., 7th Floor
Tampa, FL 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402
jyanchunis@ForThePeople.com
rmaxey@ForThePeople.com

Attorneys for Plaintiff

THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

KAMAL BITMOUNI, on behalf of himself and all others similarly situated,

Plaintiff,

vs.

PAYSAFE LIMITED, a Bermuda limited company f/k/a Paysafe Group Holdings Limited,

Defendant.

Case No.: _____

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Kamal Bitmouni ("Plaintiff"), individually and on behalf of all others similarly situated, brings this Class Action Complaint against Paysafe Limited ("Paysafe" or "Defendant"), and alleges, upon personal knowledge as to his own actions and his counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personal identifiable information that Defendant required from its customers as a condition of providing online payment services, including without limitation, names, contact details, Social Security numbers, and bank account information (collectively, "personal identifiable information" or "PII"). Plaintiff also alleges Defendant failed to provide timely, accurate, and adequate notice to Plaintiff and similarly situated current and former customers (collectively, "Class Members") that their PII had been lost and precisely what types of information was unencrypted and in the possession of unknown third parties.

2. Defendant provides merchant services to individuals and businesses throughout the United States. These services include, among other things, providing the ability to accept payments online. To obtain merchant services, Plaintiff and other customers of Defendant entrust and provide to Defendant an extensive amount of PII, including but not limited to Social Security numbers and bank account numbers. Defendant retains this information on computer hardware—even after the customer relationship ends. Defendant asserts that it understands the importance of protecting information.

3. On or before November 6, 2020, Defendant determined that there had been a potential compromise of a website used by part of its U.S. business (the "Data Breach").

4. On or before December 3, 2020, Defendant determined that suspicious activity on the website from May 13, 2018 to November 24, 2020 may have compromised information held on the website.

5. In a "Notice of Data Breach," dated December 16, 2020, Defendant advised that it was informing current and former customers of Defendant of the Data Breach.

6. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class

Members' PII, Defendant assumed legal and equitable duties to those individuals. Defendant admits that the unencrypted PII exposed to "unauthorized activity" included names, contact details, Social Security numbers, and bank account information.

7. The exposed PII of Defendant's current and former customers can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Defendant's current and former customers face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

8. This PII was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect PII of its current and former customers. In addition to Defendant's failure to prevent the Data Breach, after discovering the breach, Defendant waited over a month to report it to the states' Attorneys General and affected individuals.

9. As a result of this delayed response, Plaintiff and Class Members had no idea their PII had been compromised, and that they were, and continue to be, at significant risk to identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

10. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of their current and former customers; (ii) warn its current and former customers of its inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

11. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and significantly (iv) the continued and certainly an increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in

Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the PII.

12. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that its current and former customers' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

13. Plaintiff Kamal Bitmouni is a Citizen of California residing in Chino Hills, California. Mr. Bitmouni received Defendant's *Notice of Data Breach*, dated December 16, 2020, on or about that date.

14. Defendant Paysafe Limited, formerly known as Paysafe Group Holdings Limited, is a limited company organized under the laws of Bermuda, headquartered at Victoria Place, 21 Victoria Street, Hamilton H10, Bermuda.

15. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

16. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

17. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the

proposed class, and at least one other Class Member (including named Plaintiff Kamal Bitmouni, a Citizen of California) is a citizen of a State and Defendant is a citizen or subject of a foreign state, establishing minimal diversity.

18. The Northern District of California has personal jurisdiction over Defendant named in this action because Defendant conducts substantial business in California and this District through its subsidiaries, including but not limited to the fact that Defendant (formerly known as Paysafe Group Holdings Limited) filed a notice of the breach underlying this action with the State of California Department of Justice; and Defendant (formerly known as Paysafe Group Holdings Limited) sent notices of the breach to affected individuals in California, stating that the website compromised in the Data Breach was used by part of Defendant's United States business and that the affected individuals provided their information to "Merchant Services," which includes "Paysafe," "in the course of enrolling for a merchant account."[1]

19. Venue is proper in this District under 28 U.S.C. §1391(b) because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District, including that the website compromised in the Data Breach was used by part of Defendant's United States business and the affected individuals provided their information to "Merchant Services," which includes "Paysafe," "in the course of enrolling for a merchant account."[2]

IV. FACTUAL ALLEGATIONS

Background

20. Defendant provides various merchant products and services, including the ability to accept cash payments online; the ability to accept payments from digital wallets; customized, integrated payments merchants' software; simplified, secure e-commerce solutions for online payments; and stand alone and integrated point-of-sale products.[3]

21. Plaintiff and Class Members that used Defendant's products or services were

[1] *See Notice of Data Breach*, a true and correct copy of which is attached hereto as Exhibit 1 ("Ex. 1") (downloaded from https://oag.ca.gov/ecrime/databreach/reports/sb24-197247 on Jan. 25, 2021).

[2] *Id.*

[3] *See* Paysafe Group, *Our Story, available at*: https://www.paysafe.com/us-en/about/our-story/ (last accessed Jan. 26, 2021).

required to provide some of their most sensitive and confidential information, including names, contact details, Social Security numbers, and bank account information, and other personal identifiable information, which is static, does not change, and can be used to commit myriad financial crimes.

22. Plaintiff and Class Members, as current and former customers, relied on this sophisticated Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Defendant's current and former customers demand security to safeguard their PII.

23. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII from involuntary disclosure to third parties.

The Data Breach

24. Beginning on or about December 14, 2020, Defendant sent its current and former customers a *Notice of Data Breach*.[4] Defendant informed the recipients of the notice that:

> We are writing to inform you of a cybersecurity incident that may have affected personal information related to you. You provided the information to Merchant Services* in the course of enrolling for a merchant account.
>
> **WHAT HAPPENED** On November 6, 2020, through Merchant Services'* internal cybersecurity program, we discovered a potential compromise of a website used by part of our U.S. business. We promptly initiated an investigation to determine the nature and potential impact of the vulnerability. In the course of doing so, we identified suspicious activity indicating that an unauthorized actor submitted automated queries to the website. We created a secure environment to test the queries, using available logs and other information to assess potential impact. By November 19, 2020, we determined that a subset of the queries identified might have involved data held on the website. We analyzed logs and other information available to assess whether those queries could have returned information to unauthorized actors, and we engaged external forensics experts to assist. By December 3, 2020, we determined that some queries may have compromised certain information held on the website, although the evidence is not conclusive. At this time, we have identified evidence of suspicious

[4] *Id.*

> activity on the website between May 13, 2018, and November 24, 2020. We have notified law enforcement. Although we are not aware of any evidence confirming that the activity resulted in unauthorized actors acquiring or misusing your personal information, we are providing this notice out of an abundance of caution so that you can take steps to protect yourself.
>
> **WHAT INFORMATION WAS INVOLVED** The information about you that may have been accessed includes your name, contact details, Social Security number, and bank account information. The website did not hold customer transaction data, consumer data, or payment card information. The website impacted is separate from Merchant Services'* core processing and operating systems. The website was part of a legacy system used internally and by a small group of former Chi Payment agents, a group acquired in an acquisition of iPayment in 2018, and contains certain data of a limited subset of merchants and agents.[5]

25. On or about December 14, 2020, Defendant began notifying various state Attorneys General, including California's Attorney General Xavier Becerra, signed by "Merchant Services."[6]

26. Defendant admitted in the *Notice of Data Breach* and the letters to the Attorneys General that one or more unauthorized third persons submitted automated queries to Defendant's website and that some of these queries could have returned information to unauthorized actors, including the names, contact details, Social Security numbers, and bank account information of Defendant's current and former customers.

27. In response to the Data Breach, Defendant claims that it "took steps to prevent further unauthorized access and have closed the website. We continue to invest in cybersecurity, including enhancing our website scanning practices and vulnerability detection program. Additionally, we have arranged for you to obtain credit monitoring and identity monitoring services at no cost to you for two years through Kroll, a leading provider of credit monitoring and identity monitoring services."[7]

28. Plaintiff's and Class Members' unencrypted information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted

---

[5] Ex. 1, p.1.
[6] Ex. 2 (screenshot from State of California Department of Justice website taken Jan. 26, 2021).
[7] Ex. 1 (*Notice of Data Breach*) at 1.

marketing without the approval of the affected current and former customers. Unauthorized individuals can easily access the PII of Defendant's current and former customers.

29. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for current and former customers, causing Plaintiff's and Class Members' PII to be exposed.

Defendant Acquires, Collects and Stores Plaintiff's and Class Members' PII.

30. Defendant acquired, collected, and stored its current and former customers PII.

31. As a condition of obtaining merchant services from Defendant, Defendant requires that its customers entrust Defendant with highly confidential PII.

32. By obtaining, collecting, and storing Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

33. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and the Class Members, as current and former customers, relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Securing PII and Preventing Breaches

34. Defendant could have prevented this Data Breach by properly securing and encrypting Plaintiff's and Class Members' PII. Or Defendant could have destroyed the data, especially old data from former customers that Defendant had no legal duty to retain.

35. Defendant's negligence in safeguarding its current and former customers' PII is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

36. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and the proposed Class from being compromised.

37. The Federal Trade Commission ("FTC") defines identity theft as "a fraud

committed or attempted using the identifying information of another person without authority."[8] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[9]

38. The ramifications of Defendant's failure to keep secure its current and former customers' PII are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

39. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[10] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[11] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[12]

40. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

---

[8] 17 C.F.R. § 248.201 (2013).

[9] *Id.*

[10] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Jan. 25, 2021).

[11] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Jan. 25, 2021).

[12] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Jan. 25, 2021).

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[13]

41. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

42. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[14]

43. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number, driver's license number or government-issued identification number, name, and date of birth.

44. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the

---

[13] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Jan. 25, 2021).

[14] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthems-hackers-has-millionsworrying-about-identity-theft (last accessed Jan. 25, 2021).

black market."[15]

45. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

46. The PII of Plaintiff and Class Members was taken by hackers to engage in identity theft or and or to sell it to others criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

47. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[16]

48. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding its current and former customers' PII, including Social Security numbers and dates of birth, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Defendant's current and former customers as a result of a breach.

49. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

50. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to potentially thousands or tens or

---

[15] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Jan. 25, 2021).

[16] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed Jan. 25, 2021).

hundreds of thousands of individuals' detailed, personal information and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

51. To date, Defendant has offered its current and former customers only two years of identity theft protection services through a single credit monitoring and identity monitoring service, Kroll. The offered service is inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

52. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of its current and former customers.

Plaintiff Kamal Bitmouni's Experience

53. Beginning in or about September 2020, Plaintiff Kamal Bitmouni operated an online business that used Defendant's services to accept payment card payments. Defendant required that he provide his PII, including but not limited to his name, contact details, Social Security number, and bank account information.

54. Mr. Bitmouni received the Notice of Data Breach, dated December 16, 2020, on or about that date.

55. On or about December 5, 2020, unknown, unauthorized third-parties used Mr. Bitmouni's PII, including but not limited to his name, bank account details and Social Security number, to access his checking account – the same account used for his online business – in an attempt to divert Mr. Bitmouni's funds.

56. As a result of the Data Breach notice and the unauthorized access to his checking account, Mr. Bitmouni spent time dealing with the consequences of the Data Breach, which includes time spent communicating with his bank to stop the fraudulent transfers, verifying the legitimacy of the Notice of Data Breach, exploring credit monitoring and identity theft insurance options, signing up and routinely monitoring the credit monitoring offered by Defendant, and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

57. Additionally, Mr. Bitmouni is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

58. Mr. Bitmouni stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

59. Mr. Bitmouni suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that Mr. Bitmouni entrusted to Defendant for its services to accept payment card payments, which was compromised in and as a result of the Data Breach.

60. Mr. Bitmouni suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

61. Mr. Bitmouni has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security number, in combination with his name and bank account information, being placed in the hands of unauthorized third-parties and possibly criminals.

62. Mr. Bitmouni has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

63. The credit monitoring service provided by Defendant to Mr. Bitmouni warned him on or about January 13, 2021, that his PII is potentially exposed on the dark web.

V. CLASS ALLEGATIONS

64. Plaintiff brings this nationwide class action on behalf of himself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

65. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> All individuals whose PII was compromised in the data breach first announced by Defendant on or about December 16, 2020 (the "Nationwide Class").

66. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff Kamal Bitmouni asserts claims on behalf of a separate statewide

subclass, defined as follows:

> All individuals who are residents of California and whose PII was compromised in the data breach first announced by Defendant on or about November 16, 2020 (the "California Class").

67. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

68. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

69. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class (the "Class") are so numerous that joinder of all members is impracticable. Defendant has identified thousands of current and former customer whose PII may have been improperly accessed in the Data Breach, and the Class is apparently identifiable within Defendant's records.

70. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendant had a duty not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had a duty not to use the PII of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual, damages, and/or statutory damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

71. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

72. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members, and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

73. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

74. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

75. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

76. The litigation of the claims brought herein is manageable. Defendant's uniform

conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

77. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

78. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

79. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

80. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members; and,

i. Whether Class Members are entitled to actual damages, statutory damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

81. Plaintiff and Class Members re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 80.

82. As a condition of obtaining merchant services from Defendant, Defendant's current and former customers were obligated to provide Defendant with certain PII, including their names, contact details, Social Security numbers, and bank account information.

83. Plaintiff and the Class Members entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

84. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

85. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of its current and former customers' PII involved an unreasonable risk of harm to Plaintiff and Class Members, even if the harm occurred through the criminal acts of a third party.

86. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiff's and Class Members' information in

Defendant's possession was adequately secured and protected.

87. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former customers' PII they were no longer required to retain pursuant to regulations.

88. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class Members' PII.

89. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and Class Members. That special relationship arose because Plaintiff and Class Members entrusted Defendant with their confidential PII, a necessary part of obtaining merchant services from Defendant.

90. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or Class Members.

91. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class Members was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

92. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

93. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendant's misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decision not to comply with industry standards for the safekeeping of Plaintiff's and Class Members' PII, including basic encryption techniques freely available to Defendant.

94. Plaintiff and the Class Members had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

95. Defendant was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

96. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

97. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and Class Members.

98. Defendant has admitted that the PII of Plaintiff and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

99. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and Class Members during the time the PII was within Defendant's possession or control.

100. Defendant improperly and inadequately safeguarded the PII of Plaintiff and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

101. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect its current and former customers' PII in the face of increased risk of theft.

102. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its current and former customers' PII.

103. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove former customers' PII it was no longer required to retain pursuant to regulations.

104. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and Class Members the existence and scope of the Data Breach.

105. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class Members, the PII of Plaintiff and Class Members would not have been compromised.

106. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and Class Members and the harm suffered or risk of imminent harm suffered by Plaintiff and the Class. Plaintiff's and Class Members' PII was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

107. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

108. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

109. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

110. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

111. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

112. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and

attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the current and former customers' PII in its continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

113. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

114. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class)

115. Plaintiff and Class Members re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 80.

116. Defendant required Plaintiff and Class Members to provide their personal information, including names, contact details, Social Security numbers, and bank account information, and other personal information as a condition of obtaining merchant services from Defendant.

117. As a condition of Plaintiff and Class Members obtaining merchant services from Defendant, they provided their personal information to Defendant. In so doing, Plaintiff and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been breached, compromised, or stolen.

118. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

119. Defendant breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect their personal information and by failing to provide timely and accurate notice to them that personal information was compromised as a result of the data breach.

120. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and Class Members have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

COUNT III
Invasion of Privacy
(On Behalf of Plaintiff and the Nationwide Class)

121. Plaintiff and Class Members re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 80.

122. Plaintiff and Class Members had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

123. Defendant owed a duty to its current and former customers, including Plaintiff and

Class Members, to keep their PII contained as a part thereof, confidential.

124. Defendant failed to protect and released to unknown and unauthorized third parties the PII of Plaintiff and Class Members.

125. Defendant allowed unauthorized and unknown third parties access to and examination of the PII of Plaintiff and Class Members, by way of Defendant's failure to protect the PII.

126. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiff and Class Members is highly offensive to a reasonable person.

127. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their PII to Defendant as part of obtaining merchant services from Defendant, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

128. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

129. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that their information security practices were inadequate and insufficient.

130. Because Defendant acted with this knowing state of mind, they had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and Class Members.

131. As a proximate result of the above acts and omissions of Defendant, the PII of Plaintiff and Class Members was disclosed to third parties without authorization, causing Plaintiff and Class Members to suffer damages.

132. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

COUNT IV
Breach of Confidence
(On Behalf of Plaintiff and the Nationwide Class)

133. Plaintiff and Class Members re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 80.

134. At all times during Plaintiff's and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' PII that Plaintiff and Class Members provided to Defendant.

135. As alleged herein and above, Defendant's relationship with Plaintiff and Class Members was governed by terms and expectations that Plaintiff's and Class Members' PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

136. Plaintiff and Class Members provided their PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII to be disseminated to any unauthorized third parties.

137. Plaintiff and Class Members also provided their PII to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that PII from unauthorized disclosure.

138. Defendant voluntarily received in confidence Plaintiff's and Class Members' PII with the understanding that PII would not be disclosed or disseminated to the public or any unauthorized third parties.

139. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiff's and Class Members' PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

140. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class Members have suffered damages.

141. But for Defendant's disclosure of Plaintiff's and Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' PII as well as the resulting damages.

142. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' PII. Defendant knew or should have known its methods of accepting and securing Plaintiff's and Class Members' PII was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff's and Class Members' PII.

143. As a direct and proximate result of Defendant's breach of their confidence with Plaintiff and Class Members, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of current and former customers; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the

impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

144. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT V
Violation of California's Unfair Competition Law
(Cal. Bus. & Prof. Code § 17200, *et seq.*)
(On Behalf of Plaintiff and the Nationwide Class)

145. Plaintiff and Class Members re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 80.

146. By reason of the conduct alleged herein, Defendant engaged in unlawful and unfair business practices within the meaning of California's Unfair Competition Law ("UCL"), Business and Professions Code § 17200, *et seq*.

147. Defendant stored the PII of Plaintiff and Class Members in its computer systems. Defendant falsely represented to Plaintiff and Class Members that their PII was secure and would remain private.

148. Defendant knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with federal regulations and that would have kept Plaintiff's and Class Members' PII secure and prevented the loss or misuse of that PII.

149. Even without these misrepresentations, Plaintiff and Class Members were entitled to assume, and did assume, that Defendant would take appropriate measures to keep their PII safe. Defendant did not disclose at any time that Plaintiff's and Class Members' PII was vulnerable to hackers because Defendant's data security measures were inadequate and outdated, and Defendant was the only one in possession of that material information, which it had a duty to disclose.

A. Unlawful Business Practices

150. As noted above, Defendant violated Section 5(a) of the FTC Act (which is a predicate legal violation for this UCL claim) by misrepresenting, both by affirmative conduct and

by omission, the safety of its computer systems, specifically the security thereof, and its ability to safely store Plaintiff's and Class Members' PII.

151. Defendant also violated Section 5(a) of the FTC Act by failing to implement reasonable and appropriate security measures or follow industry standards for data security, and by failing to timely` notify Plaintiff and Class Members of the Data Breach.

152. If Defendant had complied with these legal requirements, Plaintiff and Class Members would not have suffered the damages related to the Data Breach, and consequently from Defendant's failure to timely notify Plaintiff and Class Members of the Data Breach.

153. Defendant's acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, *inter alia*, Section 5(a) of the FTC Act.

154. Plaintiff and Class Members suffered injury in fact and lost money or property as the result of Defendant's unlawful business practices. In addition, Plaintiff's and Class Members' PII was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiff and Class Members have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

B. Unfair Business Practices

155. **Defendant engaged in unfair business practices under the "balancing test."** The harm caused by Defendant's actions and omissions, as described in detail above, greatly outweigh any perceived utility. Indeed, Defendant's failure to follow basic data security protocols and misrepresentations to current and former customers about Defendant's data security cannot be said to have had any utility at all. All of these actions and omissions were clearly injurious to Plaintiffs and Class Members, directly causing the harms alleged below.

156. **Defendant engaged in unfair business practices under the "tethering test."** Defendant's actions and omissions, as described in detail above, violated fundamental public policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to

them . . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the law.

157. **Defendant engaged in unfair business practices under the "FTC test."** The harm caused by Defendant's actions and omissions, as described in detail above, is substantial in that it affects thousands of Class Members and has caused those persons to suffer actual harms. Such harms include a substantial risk of identity theft, disclosure of Plaintiff's and Class Members' PII to third parties without their consent, diminution in value of their PII, consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures. This harm continues given the fact that Plaintiff's and Class Members' PII remains in Defendant's possession, without adequate protection, and is also in the hands of those who obtained it without their consent. Defendant's actions and omissions violated Section 5(a) of the Federal Trade Commission Act. *See* 15 U.S.C. § 45(n) (defining "unfair acts or practices" as those that "cause[ ] or [are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition"); *see also, e.g.*, *In re LabMD, Inc.*, FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016) (failure to employ reasonable and appropriate measures to secure personal information collected violated § 5(a) of FTC Act).

158. Plaintiff and Class Members suffered injury in fact and lost money or property as the result of Defendant's unfair business practices. Plaintiff and Class Members' PII was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiff and Class Members have also suffered consequential out of pocket losses for procuring credit freeze or protection services,

identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

159. As a result of Defendant's unlawful and unfair business practices in violation of the UCL, Plaintiff and Class Members are entitled to damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT VI
Violation of California's Consumer Privacy Act
(Cal. Civ. Code § 1798.150)
(On behalf of Plaintiff and the California Class)

160. Plaintiff and California Class members re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 80.

161. Defendant violated section 1798.150(a) of the California Consumer Privacy Act ("CCPA") by failing to prevent Plaintiff's and California Class members' PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Plaintiff and California Class members.

162. As a direct and proximate result of Defendant's acts, Plaintiff's and California Class members' PII was subjected to unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violation of the duty.

163. As a direct and proximate result of Defendant's acts, Plaintiff and California Class members were injured and lost money or property, including but not limited the loss of California Class members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

164. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff's and California Class members' PII and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Plaintiff and California Class members.

165. Defendant is a corporation organized for the profit or financial benefit of its owners, with annual gross revenues exceeding $25 million, and collects PII as defined in Cal. Civ. Code § 1798.140.

166. Plaintiff and California Class members seek relief under § 1798.150(a), including, but not limited to, recovery of actual damages; injunctive or declaratory relief; any other relief the court deems proper; and attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5).

167. Plaintiff and the California Class members reserve the right to amend this Complaint as of right to seek statutory damages and relief under Cal. Civ. Code § 1798.100, *et seq.*

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class and the California Class as defined herein, and appointing Plaintiff and their Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and the Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying

information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff's and Class Members' personal identifying information;

v. prohibiting Defendant from maintaining Plaintiff's and Class Members' personal identifying information on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: January 27, 2021

Respectfully Submitted,

By: */s/ M. Anderson Berry*

M. Anderson Berry (SBN 262879)
Leslie Guillon (SBN 222400)
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829
aberry@justice4you.com
lguillon@justice4you.com

JOHN A. YANCHUNIS
(*Pro Hac Vice application forthcoming*)
RYAN D. MAXEY
(*Pro Hac Vice application forthcoming*)
MORGAN & MORGAN
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jyanchunis@ForThePeople.com
rmaxey@ForThePeople.com